

Cloud technology to ensure the protection of fundamental methods and use of information

Mamarajabov Odil Elmurzayevich¹

¹*Teacher of the Department of Information Technology, Tashkent State Pedagogical University named after Nizami*

ABSTRACT

A comparative analysis of attacks carried out in cloud technologies, the main methods and methods of information protection, the possibilities of using hardware and software, and methods to combat threats when eliminating them, ensuring data protection were carried out

Keywords: Cloud, Cloud Technology, Cloud Computing, Cloud Security, Authentication, Host, Active Directory, Hypervisor, Cross Site Quality

1. INTRODUCTION

Cloud technology is a model that provides IT to the consumer as a service over the Internet. The importance of "virtualization" technologies in the emergence of cloud computing is very high. The term virtualization was long forgotten after 1960 when virtualization technology was first proposed by IBM but expensive mainframe computer technology switched to cheaper x86 processor computer servers. The situation began to change in 2000, when VMware gained a monopoly on x86-bit virtualization. In 2005, VMware introduced virtual machines for free using DT. In 2006, Microsoft launched the Windows version of Microsoft Virtual PC. In 2006, Amazon created the Amazon Elastic Compute Cloud by expanding virtual servers on its devices. The cloud is an innovative model (concept) of IT infrastructure organizations, consisting of separate and distributed configured hardware and network resources, software, which are located in the data center of remote providers.

Functional attacks on cloud elements. This type of attack depends on the principle of general security with a multi-layered cloud. The solution to cloud security is as follows: to protect against functional attacks, the following source of protection should be placed on each part of the cloud: for proxy - DoS - effective protection against attack, for web - server - control the integrity of pages , for server applications - screen-level applications, for MBBT - SQL - injection protection, for data storage systems - to give proper backups (backups), restrict use. The protection mechanisms listed above have been developed, but they have not yet been put together to provide comprehensive cloud protection. Therefore, when creating a cloud, integrating them into a single system will solve the problem.

2. MAIN PART

Attacks on the control system. Many virtual machines used in the cloud require separate system management. Disruption of the control system in virtual machines - causes a malfunction and blames another virtual machine by blocking one virtual machine.

One of the most effective ways to provide security in the cloud is the Cloud Security Alliance (CSA), which analyzes the following data:

Data storage. Encryption is one of the most effective ways to protect your data. The provider that allows access to the data must encrypt the customer data stored at the data center, and delete it without return if it is no longer in use.

Data security in transmission. Transfer of encrypted data can be done only after authentication. Data can be read or modified and accessed through trusted links. Such technologies are implemented in very popular algorithms and reliable protocols AES, TLS, Ipsec.

Authentication. Password protection. Tokens and certificates are the focus of great reliability. The provider must be transparent in authorizing the identification system. It uses LDAP (Light Directory Access Protocol) and SAML (Security Assertion Markup Language) protocols.

Consumer isolation. Individual use of virtual machines and virtual networks. The following technologies should be implemented in virtual networks. VPN (Virtual Private Network), VLAN (Virtual Local Area Network) and VPLS (Virtual Private LAN Service). Providers often isolate consumer data from each other due to code changes in a single application environment. This approach is risky, as it can find its way into non-standard code and use consumer data.

Information security in the use of cloud technologies

If we look at cloud technologies from a technological point of view, the performance of applications does not differ much from the performance of traditional. Business systems also run on a separate computer, and only in cloud technologies can they be virtual. The data is stored on servers, and they are divided into several compute nodes or placed on a single large server. Many experts believe that information security in cloud technologies should be built on the principle of traditional system protection.

Based on the facts, we can divide the protection of cloud technologies into two:

- equipment safety prevention;
- data security.

In order to ensure the protection of customers, the provider needs to organize the protection of its

hardware and software from unauthorized access, tampering with IT systems, code modification. In turn, the client has the ability to use encryption technology to protect it from external attacks when entering any necessary or personal information into the system.

This includes a number of security benefits in cloud technology.

The protection of cloud technologies is determined not only by the operator or the client, but also by where it is used and the type of method.

Private Cloud. Providing information security in a private cloud environment is very easy. When working with personal cloud, we can only use computing resources and data storage service models and graphics. Then all the valuable information will remain with the company. Due to strict measures, the data on the virtual desktop may not be saved when the network is turned off. A private cloud will not only be able to provide the full range of protection as well as the full functionality of the platform and applications.

The private cloud has an arsenal of code-encoded, securely differentiated, clustered, authenticated, and maximum use of audited transactions and protected data.

A modern software solution can do a lot of work, reflecting the convenience of personal use of the database system. In particular, such features give Run-Time Privilege Analysis and Data Redactions the privilege of detecting actions that are accessing and using data stored in cloud technologies. But a private cloud requires qualified personnel, which ensures the level of service to the servers, uninterrupted and efficient virtual software at work.

It also maintains the level of business applications, workflow and service demand in the cloud. There should be kata and experienced professionals in the field of cloud security. Not all companies have this situation, so one of the most common types today is social cloud technology.

Social Cloud. One of the advantages of a public cloud is that your data is transferred to another organization and at the same time ensures its transmission and storage. Because valuable data leaves the network on a regular basis, it requires additional protection. Unfortunately, social and hybrid or traditional, private cloud systems cannot provide the same level of security. That's why many angry providers have to focus on the limited activities of services to effectively implement security in the social cloud. However, many organizations prefer to choose providers to ensure cloud security. Significantly in recent years, data stored in the cloud has been weakened and feasible by users in other countries, raising fears. That's what Steve Rose, director of consulting at Verint Systems, says.

Protection technology. In the field of IT, the cloud protection strategy provides a very high level of security, while having the highest standards of personal data protection. Cloud computing always allows participants to define requirements for each component level, defining the area. The possibility of implementing such requirements is being addressed today. Emphasis should be placed on reliable deployment and use of the internship program. Ilya Trifalenkov, director of the R-Style Center for Information Security, said that the level of application software provides access to data. Only this level of application software is at the forefront of maximum risk.

The most common threats in cloud environments are the conversion of virtual machines from the operating state, changes in the network topology of the IT infrastructure using only program parameters, attacks on IT directly from network protection mechanisms tooth This risk is reduced due to the protection of the virtual environment at all stages of construction, ie: virtual infrastructure, system management and storage system, hardware, system software schedule (hypervisor).

If we look at modern solutions, it allows to create a firewall on virtual machines, which allows continuous monitoring of virtual machines. The level of service protection is protected by a firewall, operating in a cloud computing environment.

3. CONCLUSION

The firewall can be processed at the service level in accordance with the requirements of a separate network protocol, ie specialized protocols can be filtered. Cloud computing security is provided by a castle firewall, which allows free users to control the access of address information to the virtual environment. Log updates can be entered automatically or manually. The level of protection provided by the segment AIS hardware or personal firewall. Depending on the network reliability requirements, high reliability, a separate firewall, a firewall with user workstations, a group can be used.

REFERENCES:

1. Khasanov A.A. (2018). Didactic Foundations of Interdisciplinary Connections at Subject Teaching. Eastern European Scientific Journal, Germany -2018. No. 6, pp. 127-130.
2. Khasanov A.A. (2017). Methods and methods of forming economic education through interdisciplinary communication through information technology. Education, Science and Innovation. Spiritual-Educational, Scientific and Methodological Journal, №3, pp. 38- 44.
3. Mamarajabov O.E. Abdurazzoqov J.A. The benefits of using information technology in the education system // European Journal of Research and Reflection in Educational Sciences Vol. 7 No. 12, 2019. P.446-450
4. Pulatova N.R., & Khasanov, A.A. (2019). Role of innovation in school development. European Journal of Research and Reflection in Educational Sciences, Vol. 7 No. 12, pp.502-504.

5. Urokova Sh., & Tuhtashev U. (2019). Trends of electronic education development. European Journal of Research and Reflection in Educational Sciences, Vol. 7 No. 12, pp. 768-771.
6. Hasanov A.A., & Gatiyatulina R.M. (2016). Interdisciplinary communication as a didactic conditions of increase of efficiency of educational process. Eastern European Scientific Journal Germany. Auris - kommunikations-Und verlagsgesellschaft mdh 5-2016, pp.107-111.